## Appendix C. Checklist Program Operational Procedures

National Institute of Standards and Technology

# Operational Procedures for The NIST National Checklist Program for Information Technology Products

## Version 1.2

This document sets forth the policies, procedures and general requirements for the NIST National Checklist Program for Information Technology Products. This document is intended for those individuals in developer organizations who would need to formally agree to the program's requirements.

This document is organized as follows:

- Section 1 – general considerations for the NIST National Checklist Program
- Section 2 – procedures for initial screening of a checklist prior to public review
- Section 3 – procedures for the public review of a candidate checklist
- Section 4 – final acceptance procedures
- Section 5 – maintenance and delisting procedures
- Section 6 – record keeping

The following terminology is used in this appendix:

- *Candidate* is a checklist that has been screened and approved by NIST for public review.
- *FCL* refers to the final checklist list—the listing of all final checklists on the NIST repository.
- *Final* is a checklist that has completed public review, has had all issues addressed by the checklist developer and NIST, and has been approved for listing on the repository according to the procedures of this section.

- *Checklist* is a *Technical Configuration Checklist*, which is a checklist that refers to a specific product and version.
- *Checklist Developer* or *Developer* is an individual or organization that develops and owns a checklist and submits it to the National Checklist Program.
- *Independent Qualified Reviewers* are tasked by NIST with making a recommendation to NIST regarding public review or listing of the checklist. They work independently of other reviewers and are considered expert in the technology represented by the checklist.
- *Logo* refers to the NIST National Checklist Program logo.
- *National Checklist Program*, *Program*, or *NCP* is used in place of the NIST National Checklist Program for Information Technology Products.
- *NIST Checklist Repository* or *Repository* refers to the website that maintains the checklists, the descriptions of the checklists, and other information regarding the National Checklist Program.
- *Public Reviewer* is any member of the general public who reviews a candidate checklist and sends comments to NIST.
- *Operational Environments* refer to the operational environments outlined in this document.

References to documents that form a basis for the requirements of this program are as follows:

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- NIST SP 800-27 Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), *Revision A,* http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
- NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf
- NIST SP 800-70 Revision 2, *National Checklist Program for IT Products*, http://csrc.nist.gov/publications/PubsSPs.html

## 1. Overview and General Considerations

This section focuses on general considerations for all parts of the National Checklist Program.

(a) **Checklist Lifecycle Overview:** Checklists typically have the following lifecycle:

1. Checklist developers inquire about the program and download a submission package. The developer subsequently contacts NIST with a tested checklist, supporting information, and a signed agreement to the requirements of the NCP. General information about checklists is discussed in Section 1. Checklist submission requirements and procedures are discussed in Section 2.
2. NIST verifies that all information is complete and performs a screening on the checklist. Checklists meeting the requirements for listing receive further consideration and are referred to as "candidate checklists." Section 2 discusses screening criteria and procedures. Section 1d discusses issue resolution processes.

3. NIST lists the candidate checklist on the repository for public review, typically for a period of 30 to 60 days, as discussed in Section 3.
4. NIST forwards comments from public reviewers to the developer. When all issues are addressed, the checklist is listed on the FCL, as discussed in Section 4.
5. The developer contacts NIST on typically an annual basis to determine whether the listing should continue, be updated, or be archived, as discussed in Section 5.

(b) **Intellectual Property Rights:** Developers retain intellectual property rights to their checklists.

(c) **Confidential Information:** NIST does not anticipate the need to receive confidential information from checklist developers. If it becomes necessary to disclose confidential information to NIST, NIST and the developer must enter into a separate confidentiality agreement prior to such disclosure.

(d) **Independent Qualified Reviewers:** NIST may decide to seek technical advice from independent qualified experts who will review checklist submissions to determine whether they meet the program requirements. The reviewers are tasked with making a recommendation to NIST regarding a subsequent public review or final listing of the checklist. Typical but not exclusive of the reasons for using independent reviewers include the following:

1. NIST does not possess the expertise to determine whether issues have been addressed satisfactorily.
2. NIST disagrees with proposed issue resolutions.

(e) **Terminating Consideration of a Checklist Submission:** NIST or the developer may terminate consideration of checklist submissions at any time. If NIST terminates consideration, the points of contact are asked to respond within 10 business days. Typical but not exclusive of the reasons for terminating consideration of checklist submissions include the following:

1. The submission package does not meet the screening criteria.
2. The developer fails to address issues raised at other times.
3. The developer violates the terms and conditions of participation in the program.

## 2. Checklist Submission and Screening

This section outlines the procedures and requirements for submitting checklists to NIST and the process by which NIST determines if checklists are suitable for public review. When checklists meet the screening criteria, they receive further consideration in a public review and are referred to as "candidate checklists." NIST then follows the subsequent procedures.

(a) **Notification of Checklist Program Requirements:** NIST maintains on the repository a complete set of information for developers. The information outlines the requirements for participation in the program and describes materials and timeframes.

(b) **Materials Required From the Developer:** Developers provide the following information:

1. Contact information for an individual from the submitting organization who will serve as the point of contact for questions and comments pertaining to the checklist, and contact information for a backup or deputy point of contact. The information must include postal address, direct telephone number, facsimile number, and email address.
2. The checklist, documentation, and description template.
3. The participation agreement, which must be printed, signed, and sent to NIST. NIST accepts emailed PDF copies of the participation agreement, facsimiles, or copies via regular mail.
4. Participation fees. Currently, there is no fee to checklist developers. NIST reserves the right to charge fees for participation in the future. Fees are not retroactive.

(c) **Preliminary Screening Checklist Contents:** NIST performs a preliminary screening to verify that checklists meet the program requirements. The following paragraphs summarize the screening criteria, which are described more fully in NIST Special Publication 800-70 Revision 2.

1. The checklist settings reflect consideration of recommended security and engineering practices.
2. The checklist contains a complete, clear, and concise description of the configuration settings.
3. The checklist has been tested and configuration or compatibility issues have been identified.
4. The documentation explains how to install and uninstall the checklist.
5. Checklist-related help is available.

### 3. Candidate Checklist Public Review

NIST follows the subsequent procedures when listing candidate checklists for public review.

(a) **Public Review Period:** NIST typically lists candidate checklists for a 30 to 60 day comment period. NIST reserves the right to extend the review cycle, particularly for long or complicated checklists. NIST uses the following disclaimer (or very similar words) in conjunction with candidate checklists:

> *NIST does not guarantee or warrant the checklist's accuracy or completeness. NIST is not responsible for loss, damage, or problems that may be caused by using the checklist.*

(b) **Accepting Comments from Reviewers:** Public reviewers complete a web-based feedback form to capture their comments as well as other information about the reviewer's test environment, procedures, and other relevant information. The contents of the feedback forms are considered public records.

(c) **Maintaining Records:** NIST maintains copies of all correspondence and feedback between the public and developers by creating a unique email address for each checklist. NIST will archive the information.

(d) **Addressing Comments:** At the end of the public review period, NIST announces that the comment period is closed. Depending on the number of comments received and the ramifications of those

comments to the checklist settings, NIST determines a timeframe in which the developer must respond to comments. This timeframe typically ranges from 15 to 30 days from the date the comments were submitted or from the end of the review period. At no time will this period be less than 15 days.

### 4. Final Checklist Listing

After NIST determines that a checklist and the associated developers have met all requirements for final listing, NIST lists checklists in the FCL and refers to them as "final checklists." NIST then follows the subsequent procedures.

(a) **Finalizing Checklists:** NIST lists the checklist in the FCL. NIST may send announcements to various email lists maintained by NIST or other organizations. NIST uses the following disclaimer (or very similar words) for final checklists:

> *NIST does not guarantee or warrant the checklist's accuracy or completeness. NIST is not responsible for loss, damage, or problems that may be caused by using the checklist.*

(b) **Handling Comments:** NIST continues to accept comments about final checklists by maintaining a central email address on the repository. NIST lists the procedures to be used for contacting the developer, along with the contact information for the developer, such as an email address or URL.

(c) **Scheduling Periodic Reviews:** NIST determines whether a final checklist should be reviewed periodically and typically sets a review timeframe of one year. NIST may request that a checklist be reviewed sooner for reasons such as new vulnerabilities or threats. NIST schedules reviews with the developer's points of contact. If at any time the point of contact changes, NIST must be notified immediately.

### 5. Final Checklist Update, Archival, and Delisting

NIST follows the subsequent procedures for periodic update, archival, and delisting of final checklists.

(a) **Periodic Reviews:** NIST contacts developers at least annually to identify changes in the status of checklists. NIST also may contact developers, as appropriate, to determine if there are changes in the status of a checklist, in which case developers have 30 days to respond and indicate whether checklists should be updated, archived, or delisted.

(b) **Updates:** NIST may indicate on the FCL when checklists are under periodic review. Developers have 60 days after the review to submit the updated material to NIST. Depending on the magnitude of updates, NIST may screen the checklist and schedule a public review.

(c) **Archival:** When a developer no longer provides support for the checklist, at the developer and NIST's discretion, the checklist can remain in the repository, but it will be reclassified as an archive. Typical reasons for archiving a checklist are that the product is no longer supported or is obsolete or that the developer no longer wants to provide support for the checklist.

(d) **Delisting:** NIST removes the checklist from the FCL. NIST may send announcements to various email lists maintained by NIST or other organizations.

(e) **Automatic Delisting:** If a final checklist is not reviewed annually, it is automatically removed from the FCL. At the developer and NIST's discretion, it can be reclassified as an archive.

## 6. Record Keeping

NIST maintains information associated with the program and requires that participants in the checklist program also maintain certain records, as follows.

(a) **NIST Records:** During the period that a checklist has been submitted to NIST, and during the period that a checklist is listed on the FCL as a final or archived checklist, and for three years thereafter, NIST will maintain the following:

1. The checklist description template, as listed on the repository
2. The checklist and checklist description, as listed on the repository
3. All comments submitted as part of the public review
4. All comments submitted to NIST regarding the checklist.

(b) **Developer Records:** During the period that a checklist has been submitted to NIST, and during the period that a checklist is listed on the FCL as a final or archived checklist, the developer will maintain the following:

1. The checklist description template, as listed on the repository
2. The checklist and checklist description, as listed on the repository
3. Test reports and other evidence of checklist testing.